

ALERT BULLETIN

Issue 08.08

FRAUD ALERT

Threat: ATM Skimmers
Location: Northern Virginia and Maryland

Fair Isaac's Card Alert Fraud Manager Team has been notified by a member institution that skimming equipment was placed on three different ATM locations within recent weeks. The ATMs are located in Sterling, VA; Gaithersburg, MD and Laurel, MD.

FACTS

- Placement of devices have been on Sundays with times varying from morning to early evening.
- 2 Caucasian males in their late 20's have been identified in photographs. The primary suspect is 5'8" – 6'0" in height, 165 – 185 lbs with dark hair. Both men are thin and may be wearing sunglasses in some captured images.
- Suspects place the skimming device on the ATM and then later return to retrieve it.
- Fraudulent withdrawals have almost immediately been occurring in the Ocean City, MD area. Other locations could be involved.
- A 4-door small silver car with a sun roof (possibly a Ford with Maryland plates) has been used at each location.

The following information should be considered as baseline suggestions for developing your own proactive plan for identifying and handling skimming devices if your organization deploys ATM equipment in the general vicinity.

IDENTIFYING SKIMMING DEVICES

- Perpetrators are placing skimming equipment on ATMs after hours and weekends. Physical monitoring on weekends, when possible, is suggested.
- What is your ATM supposed to look like? It is a routine practice for criminals to attach additional brochure holders to disguise wireless transmitters and batteries. Pay particular attention to the fascia of the ATM including card slot, key pad and monitor.
- If your financial institution operates ATMs in an area affected by skimming it is suggested that you instruct ATM servicing personnel to routinely and carefully examine your ATM façade for traces of adhesive, tape residue, camera tampering or unusual attachments. The presence of any of these items may indicate that the ATM has been compromised.
- Busy ATMs that suddenly have periods of downtime overnight, without being out of service, may indicate that some form of parasite was installed over the ATM, preventing its normal operation.

HANDLING SKIMMING DEVICES

- Do not disturb the crime scene. If there is a device on or inside the machine, do not touch the device in any way. Secure the perimeter around the ATM with caution tape and an out-of-order sign. Most financial institutions use a standard robbery kit that contains these items. If you do not have a kit, improvise using items at hand.
- Notify federal and local law enforcement immediately so that the ATM crime scene can be processed.
- Secure video or photos from security cameras in order to establish an accurate timeframe for the placement of the skimming devices.
- Contact your ATM Network(s) and notify them of a potential compromise.
- Request ATM transaction data to expedite notification for all external financial institutions.
- For assistance with any skimming situation please call Fair Isaac's CardAlert Fraud Manager Team directly at 1.888.440.4227 Monday through Friday 9:00 AM EST to 6:00 PM EST.
- If you have information that pertains to this case please email JohnBuzzard@fairisaac.com for further assistance in networking with other affected financial institutions or law enforcement.

888.440.4227 from the US

Investigations@FairIsaac.com email

If you would like to be removed from our distribution list please contact us via telephone or email.

Please do not post or distribute this publication without written permission from Fair Isaac Corporation.

Copyright © 2008 Fair Isaac Corporation. All rights reserved.